IT & C

ISSN 2821 - 8469, ISSN – L 2821 - 8469, Volumul 1, Numărul 2, Decembrie 2022

Proiectarea și modelarea tehnologiei blockchain - Bitcoin

Nicolae Sfetcu

Pentru a cita acest articol: Sfetcu, Nicolae (2022), Proiectarea și modelarea tehnologiei blockchain - Bitcoin, *IT & C*, **1**:2, 85-92, DOI: 10.58679/IT85290, https://www.internetmobile.ro/proiectarea-si-modelarea-tehnologiei-blockchain-bitcoin/

Publicat online: 25.08.2022

Proiectarea și modelarea tehnologiei blockchain - Bitcoin

Nicolae Sfetcu

Rezumat

Ingineria ontologică, împreună cu tehnologiile Web semantice, permit modelarea și dezvoltarea semantică a fluxului operațional necesar pentru proiectarea TB. Cel mai utilizat sistem de modelare blockchain prin reprezentarea abstractă, descrierea și definirea structurii, a proceselor, a informațiilor și a resurselor, este modelarea intreprinderilor. Modelarea intreprinderii utilizează ontologiile de domeniu folosind limbaje de reprezentare a modelului. Bitcoin este principalul sistem de plată peer-to-peer şi monedă digitală care folosește tehnologia blockchain.

Cuvinte cheie: proiectare, modelare, tehnologii, blockchain, bitcoin

Abstract

Ontology engineering, together with Semantic Web technologies, enable the semantic modeling and development of operational flow required for TB design. The most widely used blockchain modeling system by abstractly representing, describing and defining structure, processes, information and resources is enterprise modeling. Enterprise modeling uses domain ontologies using model representation languages. Bitcoin is the leading peer-to-peer payment system and digital currency that uses blockchain technology.

Keywords: design, modeling, technologies, blockchain, bitcoin

IT & C, Volumul 1, Numărul 2, Decembrie 2022, pp. 85-92
ISSN 2821 - 8469, ISSN – L 2821 - 8469
URL: https://www.internetmobile.ro/proiectarea-si-modelarea-tehnologiei-blockchain-bitcoin/



Proiectare

Ingineria ontologică, (Smith 2004) împreună cu tehnologiile Web semantice, permit modelarea și dezvoltarea semantică a fluxului operațional necesar pentru proiectarea TB. Web-ul semantic, conform W3C, "oferă un cadru comun care permite partajarea și reutilizarea datelor în limitele aplicațiilor, ale intreprinderilor și ale comunității," (W3C 2013) și deci poate fi văzut ca un integrator pentru diferite conținuturi, aplicații și sisteme de informare. Tim Berners-Lee a avut primul o viziune a puterii rețelelor de date (Berners-Lee 2007) procesate de mașini: (Berners-Lee 2004)

”Am un vis pentru Webul care devine capabil să analizeze toate datele de pe Web - conținutul, legăturile și tranzacțiile dintre oameni și computere. Un "Web semantic", care face acest lucru posibil, va apare în curând, dar atunci când se va întâmpla, mecanismele zilnice de comerț, de birocrație și din viața noastră de zi cu zi vor fi tratate de mașini care vorbesc cu

mașinile. "Agenții inteligenți" pe care oamenii i-au căutat de-a lungul veacurilor, se vor materializa în cele din urmă.” (Berners-Lee 2000)

Metadatele și tehnologiile Web semantice au permis aplicarea ontologiilor pentru proveniența cunoașterii. Cercetarea ontologică computațională poate fi utilă în plan economic (inclusiv pentru firme), social, și pentru alți cercetători, contribuind la dezvoltarea aplicațiilor specifice. (Kim and Laskowski 2016)

Mulți cercetători consideră ontologia computațională ca un fel de filozofie aplicată. (Tom Gruber 2008) În lucrarea "*Despre principiile de proiectare a ontologiilor utilizate pentru schimbul de cunoștințe*", Tom Gruber oferă o definiție deliberată a ontologiei ca termen tehnic în domeniul informaticii. (Thomas Gruber 1994) Gruber a introdus termenul ca o specificație a unei conceptualizări:

”O ontologie este o descriere (ca o specificare formală a unui program) a conceptelor și a relațiilor care pot exista formal pentru un agent sau o comunitate de agenți. Această definiție este compatibilă cu utilizarea ontologiei ca set de definiții conceptuale, dar mai general. Și este un alt sens al cuvântului decât folosirea lui în filosofie.” (Tom Gruber 1992)

În încercarea de a distanța ontologiile de taxonomii, Gruber a declarat: (Tom Gruber 1993)

”Ontologiile sunt deseori asimilate cu ierarhiile taxonomice ale clasei, definițiilor de clasă și relației de subsumare, dar ontologiile nu trebuie să se limiteze la aceste forme. Ontologiile nu se limitează, de asemenea, la definiții conservatoare - adică definiții în sens logic tradițional care introduc numai terminologia și nu adaugă nicio cunoaștere despre lume. (Enderton 2001) Pentru a specifica o conceptualizare, este necesar să se precizeze axiome care împiedică interpretările posibile pentru termenii definiți.” (Tom Gruber 1993)

Feilmayr și Wöß au rafinat această definiție: "O ontologie este o specificare formală și explicită a unei conceptualizări comune, caracterizată printr-o expresivitate semantică ridicată necesară pentru o complexitate sporită." (Feilmayr and Wöß 2016)

Una din cele mai elaborate ontologii în acest sens este ontologia trasabilității (Kim, Fox, and Gruninger 1995) care a ajutat la dezvoltarea ontologiilor TOVE pentru modelarea intreprinderilor, (Fox and Grüninger 1998) considerată ca sursă principală pentru proiectarea blockchain.

Proiectarea blockchain se bazează pe principiile fundamentale ale arhitecturii Internet: supraviețuirea (comunicațiile pe Internet trebuie să continue în ciuda pierderii de rețele sau gateway), varietatea tipurilor de servicii (mai multe tipuri de servicii de comunicații), varietatea

rețelelor (mai multe tipuri de rețele), gestionarea distribuită a resurselor, rentabilitatea, ușurința de a atașa gazdele și responsabilitatea în utilizarea resurselor. (Hardjono, Lipton, and Pentland 2018)

Modele

Cel mai utilizat sistem de modelare blockchain prin reprezentarea abstractă, descrierea și definirea structurii, a proceselor, a informațiilor și a resurselor, este modelarea intreprinderilor. (Leondes and Jackson 1992) Modelarea intreprinderii utilizează ontologiile de domeniu folosind limbaje de reprezentare a modelului. (Vernadat 1997)

Bazându-se pe proiectarea bazată pe componente, ontologia blockchain descompune blocurile în componente individuale funcționale sau logice și identifică posibilitățile, asistând în proiectarea, implementarea, și măsurarea performanțelor diferitelor arhitecturi de blocuri. (Tasca and Tessone 2017) Conform lui Paolo Tasca, abordarea metodologică este compusă în principiu din următoarele etape:

1. Studiul comparativ al diferitelor blocuri: analiza vocabularului și a termenilor pentru a rezolva ambiguitățile și dezacordurile
2. Definirea cadrului: identificarea și clasificarea componentelor, definind o ontologie ierarhică
3. Categorisirea nivelelor: sunt introduse și comparate diferite aspecte pentru componentele de la cel mai mic nivel al structurii ierarhice.

Ca orice tehnologie TIC, un blockchain este condus de principiile fundamentale ale descentralizării datelor, transparenței, securității și confidențialității. (Aste, Tasca, and Matteo 2017) Alte proprietăți fundamentale ale blockchain includ automatizarea datelor și capacitatea de stocare a datelor.

Conform lui Fox și Gruninger, dintr-o perspectivă de proiectare, un model de intreprindere ar trebui să ofere limbajul folosit pentru a defini în mod explicit o intreprindere. (Fox and Grüninger 1998) Din perspectiva operațiunilor, modelul intreprinderii trebuie să fie capabil să reprezinte ceea ce este planificat, și ceea ce s-a întâmplat, și să furnizeze informațiile și cunoștințele necesare pentru a sprijini operațiunile. (Fox and Grüninger 1998) Funcțiile sunt modelate printr-o reprezentare structurată, (FIPS PUBS 1993) o reprezentare grafică într-un domeniu definit pentru identificarea nevoilor de informare, identificarea oportunităților și determinarea costurilor. (Department Of Defense (DOD) Records Management (RM) 1995) Alte perspective pot fi cele comportamentale, organizaționale sau informaționale. (Koskinen 2000)

O modelare funcțională adecvată TB se concentrează pe proces, folosind patru simboluri în acest scop:

- Proces: Ilustrează transformarea de la intrare la ieșire.
- Stocare: Colectarea de date sau alt fel de material.
- Debit: Deplasarea datelor sau a materialelor în proces.
- Entitate externă: Externă față de sistemul modelat, dar interacționează cu acesta.

Un proces poate fi reprezentat ca o rețea a acestor simboluri. În Dynamic Enterprise Modeling (DEMO), de exemplu, o descompunere se face în modelul de control, modelul de funcții, modelul de proces și modelul organizațional.

Modelarea datelor folosește aplicarea descrierilor formale într-o bază de date. (Whitten, Bentley, and Dittman 2004) Modelul de date va consta din entități, atribute, relații, reguli de integritate și definiții ale obiectelor, fiind utilizat pentru proiectarea interfeței sau a bazei de date.

Bitcoin

Bitcoin este principalul sistem de plată peer-to-peer şi monedă digitală care folosește tehnologia blockchain. Caracteristicile rețelei Bitcoin: (Calvery 2013)

- Nu există un server central, rețeaua Bitcoin este peer-to-peer.
- Nu există un depozit central, registrul de bitcoin este distribuit.
- Registrul este public, oricine îl poate stoca pe computer.
- Nu există un administrator, registrul este menținut de o rețea de mineri la fel de privilegiați.
- Oricine poate deveni un miner.
- Adăugările la registru sunt menținute prin concurență. Până când un nou bloc nu este adăugat în registru, nu se știe care miner va crea blocul.
- Emisiunea de bitcoin este descentralizată. Aceste criptovalute sunt emise ca recompensă pentru crearea unui nou bloc.
- Oricine poate să creeze o adresă bitcoin nouă (o corespondență bitcoin a unui cont bancar) fără a avea nevoie de aprobare.
- Oricine poate trimite o tranzacție în rețea fără a avea nevoie de aprobare, rețeaua confirmă doar că tranzacția este legitimă.

Cercetătorii au subliniat o "tendință de centralizare": pe de o parte, minerii Bitcoin se alătură unor mari baze miniere pentru a minimiza varianța veniturilor lor. (Böhme et al. 2015, 215–22) Pe de altă parte, s-a format o "aristocrație" Bitcoin ca rezultat al arhitecturii codului; membrii acestei aristocrații sunt cei care au intrat devreme în jocul Bitcoin.

Nigel Dodd argumentează în *Viața socială a Bitcoin* că esența ideologiei bitcoin este de a scoate banii din controlul social, inclusiv al guvernului, existând chiar o *Declarație de independență Bitcoin*. Declarația include un mesaj al cripto-anarhismului cu cuvintele: "Bitcoin

este în mod inerent anti-instituție, anti-sistem și anti-stat. Bitcoin subminează guvernele și perturbă instituțiile, deoarece bitcoin este fundamental umanitar." (von Hayek 1976)

David Golumbia afirmă că ideile care influențează susținătorii bitcoin apar din mișcările extremiste de dreapta și retorica lor anti-banca centrală, sau, mai recent, libertarianismul lui Ron Paul și Tea Party. (The Economist 2018)

Kroll și colab. susțin că ecologia Bitcoin va avea nevoie de structuri de guvernare pentru a supraviețui, (Kroll, Davey, and Felten 2013) existând deja semne de structuri de guvernanță emergente. Aceste moduri de guvernare se pot baza pe consens și, dacă conducerea se opune, comunitatea poate să aleagă un alt curs. Dincolo de acestea, evoluțiile recente au arătat că un singur bazin minier ar putea contribui atât de mult la procesele computationale ale Bitcoin, încât ar putea controla eficient întregul sistem, punând astfel capăt structurii sale descentralizate. (Kostakis and Giotitsas 2014)

Bauwens și Kostakis susțin că Bitcoin nu este un proiect orientat spre comunitate, ci o monedă care reflectă un nou tip de capitalism - capitalismul "distribuit", (Kostakis, Bauwens, and Niaros 2015) bazat pe ideologia politică liberală care pledează pentru eliminarea statului în favoarea suveranității individuale. În practică, ceea ce se obține este un capital concentrat și o guvernare centralizată.

Vasilis Kostakis și Chris Giotitsas consideră și ei că Bitcoin exemplifică un tip derivat de "capitalism distribuit" (Kostakis and Giotitsas 2014) deși ar trebui să fie mai degrabă văzut ca o inovație tehnologică.

Bibliografie

Aste, Tomaso, Paolo Tasca, and Tiziana di Matteo. 2017. “Blockchain Technologies: The Foreseeable Impact on Society and Industry.” *Computer* 50: 18–28. https://doi.org/10.1109/MC.2017.3571064.

Berners-Lee, Tim. 2000. *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web*. HarperCollins.

———. 2004. “Semantic Web.” ResearchGate. 2004. https://www.researchgate.net/publication/307845029_Tim_Berners-Lee’s_Semantic_Web.

———. 2007. “Q&A with Tim Berners-Lee - Bloomberg.” 2007. https://www.bloomberg.com/news/articles/2007-04-09/q-and-a-with-tim-berners-leebusinessweek-business-news-stock-market-and-financial-advice.

Böhme, Rainer, Christin Nicolas, Edelman Benjamin, and Tyler Moore. 2015. “Bitcoin: Economics, Technology, and Governance.” https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.2.213.

Calvery, Jennifer Shasky. 2013. “Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury Before the United States Senate Committee on Homeland Security and Government Affairs.” https://www.fincen.gov/sites/default/files/2016-08/20131118.pdf.

Department Of Defense (DOD) Records Management (RM). 1995. “Reader’s Guide to IDEF0 Function Models.” https://www.archives.gov/files/era/pdf/rmsc-19951006-dod-rm-function-and-information-models.pdf.

Enderton, Herbert. 2001. “A Mathematical Introduction to Logic - 2nd Edition.” 2001. https://www.elsevier.com/books/a-mathematical-introduction-to-logic/enderton/978-0-08-049646-7.

Feilmayr, Christina, and Wolfram Wöß. 2016. “An Analysis of Ontologies and Their Success Factors for Application to Business.” *Data & Knowledge Engineering* 101: 1–23. https://doi.org/10.1016/j.datak.2015.11.003.

FIPS PUBS. 1993. “FIPS Publication 183 Released of IDEFØ December 1993 by the Computer Systems Laboratory of the National Institute of Standards and Technology (NIST).” http://www.idef.com/wp-content/uploads/2016/02/idef0.pdf.

Fox, Mark Stephen, and Michael Grüninger. 1998. “Enterprise Modeling.” ResearchGate. 1998. https://www.researchgate.net/publication/220604924_Enterprise_Modeling.

Gruber, Thomas. 1994. “Toward Principles for the Design of Ontologies Used for Knowledge Sharing.” ResearchGate. 1994. https://www.researchgate.net/publication/2626138_Toward_Principles_for_the_Design_of_Ontologies_Used_for_Knowledge_Sharing.

Gruber, Tom. 1992. “What Is an Ontology?” 1992. http://www-ksl.stanford.edu/kst/what-is-an-ontology.html.

———. 1993. “A Translation Approach to Portable Ontology Specifications.” 1993. http://tomgruber.org/writing/ontolingua-kaj-1993.htm.

———. 2008. “Ontology.” 2008. http://tomgruber.org/writing/ontology-definition-2007.htm.

Hardjono, Thomas, Alexander Lipton, and Alex Pentland. 2018. “Towards a Design Philosophy for Interoperable Blockchain Systems.” ResearchGate. 2018. https://www.researchgate.net/publication/325168344_Towards_a_Design_Philosophy_for_Interoperable_Blockchain_Systems.

Hayek, Friedrich von. 1976. “Denationalisation of Money: The Argument Refined.” https://nakamotoinstitute.org/static/docs/denationalisation.pdf.

Kim, Henry M., Mark S. Fox, and Michael Gruninger. 1995. “An Ontology of Quality for Enterprise Modelling.” In , 105. IEEE Computer Society. http://dl.acm.org/citation.cfm?id=832309.837247.

Kim, Henry M., and Marek Laskowski. 2016. “Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance.” *ArXiv:1610.02922 [Cs]*. http://arxiv.org/abs/1610.02922.

Koskinen, Minna. 2000. “Process Perspectives. In: Metamodeling and Method Engineering.” http://users.jyu.fi/~jpt/ME2000/Me14/sld004.htm.

Kostakis, Vasilis, Michel Bauwens, and Vasilis Niaros. 2015. “Urban Reconfiguration after the Emergence of Peer-to-Peer Infrastructure: Four Future Scenarios with an Impact on Smart Cities.” In *Smart Cities as Democratic Ecologies*, edited by Daniel Araya, 116–24. London: Palgrave Macmillan UK. https://doi.org/10.1057/9781137377203_8.

Kostakis, Vasilis, and Chris Giotitsas. 2014. "The (A)Political Economy of Bitcoin." ResearchGate. 2014. https://www.researchgate.net/publication/287241993_The_APolitical_Economy_of_Bitcoin.

Kroll, Joshua A., Ian C. Davey, and Edward W. Felten. 2013. "The Economics of Bitcoin Mining , or Bitcoin in the Presence of Adversaries." In .

Leondes, Cornelius T., and Richard Henry Frymuth Jackson. 1992. *Manufacturing and Automation Systems: Techniques and Technologies*. Academic Press.

Smith, Barry. 2004. "Beyond Concepts: Ontology as Reality Representation." In *Formal Ontology in Information Systems (FOIS)*, edited by Achille C. Varzi and Laure Vieu, 1–12.

Tasca, Paolo, and Claudio J. Tessone. 2017. "Taxonomy of Blockchain Technologies. Principles of Identification and Classification." *ArXiv:1708.04872 [Cs]*. http://arxiv.org/abs/1708.04872.

The Economist. 2018. "Bitcoin and Other Cryptocurrencies Are Useless." *The Economist*, 2018. https://www.economist.com/leaders/2018/08/30/bitcoin-and-other-cryptocurrencies-are-useless.

Vernadat, F. B. 1997. "Enterprise Modelling Languages." In *Enterprise Engineering and Integration: Building International Consensus Proceedings of ICEIMT '97, International Conference on Enterprise Integration and Modeling Technology, Torino, Italy, October 28–30, 1997*, edited by Kurt Kosanke and James G. Nell, 212–24. Research Reports Esprit. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-60889-6_24.

W3C, W3C. 2013. "W3C Semantic Web Activity Homepage." 2013. https://www.w3.org/2001/sw/.

Whitten, Jeffrey L., Lonnie D. Bentley, and Kevin C. Dittman. 2004. *Systems Analysis and Design Methods*. McGraw-Hill Irwin.